CERTIFICATE OF MAILING UNDER 37 CFR§ 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Commissioner of Patents, P.O. BOX 1450; Alexandria, VA 22313 on **December 12, 2003.**

EXPRESS MAIL LABEL: EL 113 772 037 US

Amirah Scarborough
Name of Person Mailing Document

Amirah Scarborough
Signature of Person Mailing Document

SYSTEM AND METHOD FOR PROVIDING ENDORSEMENT CERTIFICATE

I. Field of the Invention

The present invention relates generally to secure computing devices.

II. Background

Trust has become an important issue for e-commerce and other applications, particularly for mobile computing devices such as notebook computers. Specifically, as the mobility of the computing platform increases, it becomes susceptible to theft, with stolen data often representing a bigger loss than the hardware itself, because the data can include, e.g., user identity information, credit card information, and so on.

With this in mind, the Trusted Computing Platform Alliance (TCPA) has been formed to develop a specification for a trusted computing platform. Using a hardware security module (actually, a microcontroller) known as the Trusted Platform Module (TPM) that is soldered to the motherboard of the computing platform, the TCPA establishes what can be thought of as a platform root of trust that uniquely

identifies a particular platform and that provides various cryptographic capabilities including hardware-protected storage, digital certificates, IKE (Internet Key Exchange), PKI (Public Key Infrastructure), and so on. Essentially, to overcome the vulnerability of storing encryption keys, authentication certificates, and the like on a hard disk drive, which might be removed or otherwise accessed or tampered with by unauthorized people, encryption keys, certificates, and other sensitive data is stored on the secure TPM.

The various keys including the endorsement keys are unique to the TPM. The endorsement keys are either generated at manufacturing time outside the TPM and then sent ("squirted") to the TPM for storage, or the keys are generated within the TPM itself. The keys can be used to in turn encrypt other keys for various purposes, thereby extending the trust boundary as desired.

The validity of the endorsement keys is attested to by an electronic document known as an endorsement certificate that is provided by someone other than the entity that provides the keys and that is generated using the TPM public half of the endorsement key. In other words, to ensure the validity of the TPM, the user of the TPM/host device may require an endorsement certificate, a process the details of which are currently undefined. As recognized herein, the provision of the endorsement certificate must be accomplished in a way that complicates hacking or that otherwise complicates compromising the process of certifying the validity of the TPM (and, hence, that complicates unauthorized attempts to defeat the security provided by the TPM).

SUMMARY OF THE INVENTION

A method for providing an endorsement certificate to a customer computing device includes providing an endorsement key pair to a security module (such as a trusted platform module) associated with

the customer device. The endorsement key pair includes a public key and a private key. The method further includes storing data representative of the public key in a storage external to the customer device, and at a subsequent time, receiving at a comparison agent accessing the storage, certificate request data from the customer device. The comparison agent may or may not be associated with the storage agent. The certificate request data includes the public key and/or a hash of the public key with a temporary secret. It is then determined whether at least a portion of the certificate request data transmitted to the comparison agent matches the data representative of the public key stored in the storage. If so, the method includes generating the endorsement certificate using the public key and providing the endorsement certificate to the customer device. If desired, the method can also include signing the endorsement certificate with a signing key.

In another aspect, a customer device includes a security module containing a private key and a public key related to the private key, with the keys establishing an endorsement key pair. A processor accesses the security module and executes logic that includes requesting an endorsement certificate by sending data representative of the public key to a source of endorsement certificates. If it is determined at the source that the data representative of the public key matches a version of the data representative of the public key already stored at the source, the logic executed by the processor includes receiving from the source the endorsement certificate, which is generated at least in part by the public key.

In still another aspect, a computing facility includes means for storing data representative of public keys associated with respective customer computing devices, prior to providing the devices to customers. The facility also includes means for receiving transmissions of data representative of public keys from devices provided to customers, and means for comparing data representative of a public key from a device

provided to a customer with at least data representative of a public key in the means for storing to determine if a match is found. Means are provided for generating an endorsement certificate if a match is found.

In another aspect, a service includes storing data representative of public keys associated with respective customer computing devices, and receiving transmissions of data representative of public keys from customer computing devices. The service also includes comparing the received data representative of a public key with at least the stored data representative of a public key to determine if a match is found, and, if a match is found, generating an endorsement certificate that is provided to the customer computing device.

The details of the present invention, both as to its structure and operation, can best be understood in reference to the accompanying drawings, in which like reference numerals refer to like parts, and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of the present architecture; and

Figure 2 is a flow chart of the presently preferred logic.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring initially to Figure 1, a computing system is shown, generally designated 10, that includes a customer computing device or platform 12. The customer device 12 can be any suitable computer, e.g., a personal computer or larger, a laptop computer, a notebook computer or smaller, etc.

As shown in Figure 1, the preferred non-limiting customer device 12 includes a motherboard 14 on which is mounted at least one main central processing unit (CPU) 16 that can communicate with a solid state memory 18 on the motherboard 14. The memory 18 can contain basic input/output system (BIOS) instructions useful for booting the device 12 at start up. Additionally, other storage can be provided external to the motherboard 14, e.g., a hard disk drive 20 (that can hold a pre-load image of the software state of the device 12 upon completion of start up) and a floppy diskette drive 22. Moreover, the CPU 16 can communicate with external devices through a universal serial bus (USB) 24 using interface electronics 26 in accordance with USB principles known in the art.

As intended by the present invention, the customer device 12 can be rendered into a trusted device by the user. To this end, a security module such as a trusted platform module (TPM) 28 is provided on the motherboard 14. The presently preferred non-limiting TPM 28 is a hardware module that is soldered or otherwise affixed to the motherboard 14. Among other things, the TPM 28 contains various encryption keys 30, including storage keys, endorsement keys, and so on.

In accordance with the present invention, Figure 1 shows that a vendor or other facility 32 can communicate with the customer device 12 for purposes to be shortly disclosed. The facility 32 includes a key comparison database or file system 34 that is accessed by a preferably software-implemented comparison agent 36 that communicates, via a wired or wireless link 37, with the customer device 12. The

comparison agent 36 may be part of a Web interface, so that the logic below may be conducted over the Internet.

Figure 2 shows the logic of the present invention. Commencing at block 38, during manufacture of the TPM 28 an endorsement key pair (consisting of a private key and a public key) is provided to the TPM 28. The key pair may be generated outside the TPM and then "squirted" to the TPM at the time of manufacture, or the TPM itself may generate the key pair. In any case, the key pair may be generated using, e.g., a random number using public key/private key generation principles known in the art. The private key is never sent outside the TPM 28, but at block 40 the public key portion is read and stored in the database 34. Once a copy of the public key is stored in the database 34, the customer device 12 with TPM 28 may be shipped, vended, or otherwise provided to the customer at block 42.

Block 44 indicates that when the customer requires an endorsement certificate, the customer causes the device 12 to send the public key portion of the endorsement key of the TPM 28 to the comparison agent 36. As recognized by the present invention, particularly when the endorsement key pair initially is generated outside the TPM and then squirted to it, it is desirable that a temporary secret such as a nonce (e.g., a random number of around twenty bytes) also be provided in the TPM 28 and also to the comparison agent 36. In such a case, not only is the public key sent to the comparison agent 36 at block 44, but also a version of the public key as modified by the temporary secret, e.g., a SHA-1 hash of the public key and nonce. Once the request for a certificate has been sent along with the nonce/key hash, the TPM 28 destroys the nonce by, e.g., erasing it, so that the nonce cannot subsequently be discovered by de-layering the TPM 28.

At decision diamond 46 the agent determines whether the key received from the customer at block 44 matches the copy that was stored in the database 34 at block 40. When a version of the public key as hashed by the nonce is sent, the comparison agent 36 may compare a hash of the nonce and the public key in its database with the hash of the nonce and key received from the TPM 28. This comparison can be made by scanning the entire list of keys in the database 34, or by originally storing keys by TPM ID and then entering the database with the ID if provided at block 44, or by other means. In any case, if no match is found the process ends at state 48, but if a match is found, an endorsement certificate is generated at block 50 using the public key, preferably in accordance with TCPA certificate principles known in the art. If desired the certificate with key may be signed using a signing key. The certificate is then downloaded or otherwise provided to the customer at block 52.

All or portions of the above logic may be provided by a service that can be billed on an event by event basis (when a certificate is generated, e.g.) or, as another example, on a subscription basis. For instance, a service provider may access the storage, even if the storage is not maintained by the service provider, to provide certificates as set forth above.

While the particular SYSTEM AND METHOD FOR PROVIDING ENDORSEMENT CERTIFICATE as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended

to mean "one and only one" unless explicitly so stated, but rather "one or more". It is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase "means for" or, in the case of a method claim, the element is recited as a "step" instead of an "act". Absent express definitions herein, claim terms are to be given all ordinary and accustomed meanings that are not irreconcilable with the present specification and file history.